Victoria J. Maniatis, Esq.
Blake Hunter Yagman, Esq.
Gary M. Klinger*
David K. Lietz
MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, NY 11530
Telephone: (516) 741-5600
Fax: (516) 741-0128
Email:VManiatis@thesandersfirm.com
byagman@milberg.com
gklinger@milberg.com
dlietz@milberg.com
Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

DORA MICAH, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

AMERICAN FINANCIAL RESOURCES, INC.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Dorah Micah ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint (the "Action") against American Financial Resource, Inc. ("Defendant" or "AFR"), a New Jersey corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This Action arises out of the recent data breach at AFR that targeted the information of consumers who utilized AFR for residential mortgage services (the "Data Breach").

2. The Data Breach resulted in unauthorized access to the sensitive data of consumers that used AFR's services. Because of the Data Breach, thousands of Class Members' suffered ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack and the present and substantial risk of imminent harm caused by the compromise of their sensitive personal information, including their name, Social Security number and Driver's License number (hereinafter, the "Personally Identifiable Information" or "PII").

3. To compound matters, AFR's Data Breach occurred from December 6, 2021 through December 20, 2021 and AFR did not ascertain what information was accessed until February 4, 2022.

4. Then AFR sat on the information for over a month – failing to disseminate data breach consumer notifications until March 9, 2022. When a data set that is inclusive of the aforementioned PII is breached, every moment is precious to ensure that that data is not then weaponized against the rightful owner of that data through identity theft. Sitting on this information allowed AFR to dodge responsibility and inevitably worsened the Data Breach victims' chances at weathering the storm that AFR created.

5. As a result of the Data Breach, Plaintiff and Class Members have been harmed – they have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and forever closely monitor their financial accounts to guard against identity theft.

6. Plaintiff and Class Members may also incur out-of-pocket costs, for example, through having to purchase credit monitoring systems, credit freezes, or other protective measures to deter and detect identity theft. Plaintiff seeks to remedy those harms on behalf of himself and all similarly situated persons whose PII was accessed unlawfully during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

7. As such, Plaintiff brings this Action against Defendant seeking redress for its unlawful conduct, asserting claims for: (1) negligence, (2) negligence per se, (3) breach of implied contract, (4) unjust enrichment, and (5) violations of New Jersey state consumer protection statutes.

II. JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act because (1) there are more than 100 putative Class Members, (2) the aggregate amount-in-controversy, exclusive of costs and interest, exceeds $5,000,000.00, and (3) there is minimal diversity as required by the state because Plaintiff and Defendants are citizens of different states – namely, that Plaintiff is a Maryland resident and the Defendant is headquartered here, in New Jersey.

9. This Court has personal jurisdiction over the Defendant because the Defendant is from this District. Additionally, this Court has personal jurisdiction over the Defendant because they have substantial contacts with this District and have purposely availed themselves to the Courts in this District.

10. In accordance with 28 U.S.C. 1391, venue is proper in this District because a substantial part of the conduct giving rise to the Plaintiff's claims occurred in this District, the Defendant is headquartered in this District, and the Defendant transacts business within this District. In accordance with 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District and Defendant has intentionally availed themselves of the laws and markets within this District.

III. PARTIES

11. Plaintiff Dorah Micah is a resident of the state of Maryland. Plaintiff was notified of the Data Breach and her PII being compromised upon receiving the Notice letter dated March 9, 2022.

12. Defendant AFR is a domestic corporation organized under the laws of New Jersey. AFR maintains its principal place of business at 9 Sylvan Way, Parsippany, New Jersey, 07054.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

13. Defendant AFR, founded in 1997 and based in Parsippany, New Jersey, "serve[s] thousands of mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and contractors across the country with their residential financing needs."[1]

14. The way AFR does this is as follows:

a. Offering services as a "full service mortgage lender";

b. "Serving wholesale, correspondent, and consumer direct channels";

c. Offering "[d]iverse delivery options including FHA, VA, USDA, Ginnie Mae, Fannie Mae, and Freddie Mac";

[1] https://www.afrcorp.com, (last accessed Mar. 24, 2022).

d. "A top lender in 203(k) lending for sponsored originations";

e. Working as "[o]ne of the nation's leading renovation and manufactured home lenders"; and

f. Offering "an extensive program suite, eclectic channels of operations and cutting-edge technology."[2]

15. According to AFR, they are, "a group of trusted, innovative, and responsive mortgage professionals who … bring a dedicated focus to simplify the lending process."[3]

16. In the course of regular business, AFR, according to their Privacy Policy, collects and shares at least the following information:

a. Social Security number;

b. Employment information including tax returns, W-2's, pay stubs, and related documents;

c. Credit history and investment experience;

d. Current and previous home ownership experience, including physical and mailing addresses;

e. Letters of explanation regarding credit or employment events;

f. Date of birth/age; and,

g. Other information required by [AFR's] investors or insurers.[4]

17. With respect to Social Security numbers, AFR states the following in their Privacy Policy:

> Social Security numbers are classified as "Confidential" information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate

[2] *Id.*
[3] *Id.*
[4] https://www.afrcorp.com/privacy-statement/, (last accessed Mar. 24, 2022).

> business "need to know" in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers collected or retained by AFR in connection with customer, employee, or other relationships.[5]

18. And, with respect to privacy in general, the Privacy Policy states: "[AFR] has been committed to your financial well-being and protecting the privacy and security of the information you share with us since our inception in 1997."[6]

19. With respect to what information is shared, AFR states the following:

> We may share information with service providers with whom we work, such as data processors and companies that help us market products and services to you. When permitted, or required by law, we may share information with additional third parties for purposes including response to legal process.
>
> When you submit a loan application to us, we may ask for information that may include where you work, what you do, your income, assets, debts and obligations, your financial goals and other similar information. We use this information when evaluating your eligibility for a loan. This evaluation also requires us to obtain information about you from others such as consumer reporting agencies (also known as credit bureaus), the IRS, licensed title search companies, and your hazard and/or flood insurance company.
>
> In addition, American Financial Resources, Inc. may provide third party firms with information furnished by you, such as names, addresses and the financial information you have provided to us or that we have obtained from others about you. Any use of this information will be restricted to advancing your request for a loan, locating a home, or the marketing of other financial products American Financial Resources, Inc. may offer. We will never sell information about you to any other organization.
>
> We may also provide certain information to others when legally required to do so (for instance, in response to a subpoena), to prevent fraud, or to comply with a request by a government agency or regulator.

---

[5] *Id.*
[6] *Id.*

20. By obtaining, collecting, using and deriving benefits from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting said PII from unauthorized disclosure.

21. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

THE DATA BREACH

22. To define data breaches: "a data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission."[7]

23. According to AFR's Data Breach Notification, there was a security incident discovered on an unspecified date in 2021. When AFR learned of the Breach, they conducted a comprehensive review of the files--which concluded on February 4, 2022--which determined that there had been a data breach involving Plaintiff's and Class Members' PII.

24. The Data Breach itself took place between December 6, 2021 and December 20, 2021. So, for two weeks, hackers had unfettered access to AFR's trove of Personally Identifiable Information without detection.

25. However, rather than promptly inform consumers about the seriousness and the dangers, which are well known, of data breaches – and of this particular Data Breach, specifically – the Defendant opted not to inform consumers until nearly a month after the discovery of the Data Breach on March 9, 2022.

26. The Data Breach resulted in unauthorized access to the sensitive data of consumers that used AFR's services. Because of the Data Breach, thousands of Class Members' suffered

[7] "*How Data Breaches Happen*," KASPERSKY, at https://www.kaspersky.com/resource-center/definitions/data-breach (last accessed Mar. 15, 2022).

ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack and the present risk of imminent harm caused by the compromise of their sensitive personal information, including their name, Social Security number and Driver's License number.

27. The Personally Identifiable Information contained in the files accessed in the Data Breach was not encrypted.

28. While AFR stated in its "Notice" to consumers notifying them about the Data Breach that it learned of the Data Breach in early February of 2022, AFR did not begin notifying impacted victims, such as Plaintiff and members of the putative Class, until March 9, 2022 – over a month after discovering the Data Breach. AFR's delay in notifying the victims of the Data Breach violates provisions of the New Jersey Consumer Security Breach Disclosure Act, which required AFR, once it knew or had reason to know of a data security breach involving personal information of New Jersey residents, to provide prompt and direct notice of such breach to any affected New Jersey consumers.

29. Plaintiff and Class Members provided their Personally Identifiable Information to Defendant with the reasonabl expectation and the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the breach.

30. Therefore, the increase in such attacks, and the attendant risk of future attacks was widely known to the public and to anyone in the Defendant's industry, including the Defendant itself.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

31. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

32. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[8] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[9]

33. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

34. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

---

[8] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 15, 2022).

[9] *Id.*

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

35. Defendant failed to properly implement basic data security practices.

36. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Personally Identifiable Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

37. Defendant was at all times fully aware of its obligation to protect the Personally Identifiable Information of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

38. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

39. Other best cybersecurity practices that are standard in the Defendant's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

40. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

41. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANT'S BREACH

42. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;

e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

f. Failing to adhere to industry standards for cybersecurity.

43. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access AFR's IT systems which contained unsecured and unencrypted PII.

44. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

HARM TO CONSUMERS

45. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

46. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

47. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

48. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

49. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

50. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[10]

51. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[11]

52. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[12]

53. The fraudulent activity resulting from the Data Breach may not come to light for years.

54. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

55. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver's license numbers, and financial account information, and of the foreseeable

---

[10] Brian Naylor, "*Victims of Social Security Number Theft Find It's Hard to Bounce Back*," NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[11] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021).

[12] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021).

consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

56. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

HARM TO PLAINTIFF

57. Prior to the Data Breach, Ms. Micah provided her PII to AFR for purposes of obtaining a mortgage.

58. In February, 2022, Ms. Micah received Notice of Data Breach Letter from AFR informing her that her full name and social security number were stolen by cyberthieves in the Data Breach. As a result of the Data Breach, AFR directed Plaintiff to take certain steps to protect his PII and otherwise mitigate her damages.

59. As a result of the Data Breach and the directives that she received in the Notice Letter, Ms. Micah spends approximately 3-4 hours per week dealing with the consequences of the Data Breach (self-monitoring her bank and credit accounts), as well as her time spent verifying the legitimacy of the *Notice of Data Breach*, communicating with her bank, exploring credit monitoring and identity theft insurance options, signing up for the credit monitoring supplied by AFR, and reporting the breach to local law enforcement. This time has been lost forever and cannot be recaptured.

60. Ms. Micah is very careful about sharing her own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

61. Ms. Micah stores any and all documents containing PII in a secure location, and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts.

Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

62. Ms. Micah suffered actual injury and damages due to AFR's mismanagement of her PII before the Data Breach.

63. Ms. Micah suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to AFR for the purpose of providing her mortgage services, which was compromised in and as a result of the Data Breach.

64. Ms. Micah suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered anxiety and increased concerns for the theft of her privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her Social Security number.

65. Ms. Micah has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

66. Ms. Micah has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in AFR's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

67. Plaintiff brings this Action on behalf of herself and on behalf of all other persons similarly situated (the "Class"). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons who utilized AFR's services, whose Personally Identifiable Information was maintained on AFR's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class Definition").

68. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

69. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of over 10,000 individuals whose sensitive data was compromised in the Data Breach.

70. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personally Identifiable Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

e. Whether Defendant owed a duty to Class Members to safeguard their Personally Identifiable Information;

f. Whether Defendant breached a duty to Class Members to safeguard their Personally Identifiable Information;

g. Whether computer hackers obtained Class Members Personally Identifiable Information in the Data Breach;

h. Whether the Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

l. Whether Defendant failed to provide notice of the Data Breach in a timely manner;

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

71. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

72. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

73. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized

issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

74. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

75. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

76. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

77. AFR required Plaintiff and Class Members to submit non-public Personally Identifiable Information, including but not limited to, Social Security Numbers and Driver's License Numbers, as a condition of using the financial services of AFR.

78. By collecting and storing this data, and sharing it and using it for commercial gain, AFR had a duty of care to use reasonable means to secure and safeguard this information, to prevent disclosure of the information, and to guard the information from theft.

79. AFR's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

80. AFR also owed a duty of care to Plaintiff and members of the Class to provide security consistent with industry standards, and to ensure that its systems and networks and the personnel responsible for them adequately protected their customers' information.

81. Only AFR was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Class from a data breach. AFR breached its duty by failing to use reasonable measures to protect Plaintiff's and Class Members' Personally Identifiable Information.

82. The specific negligent acts and omissions committed by AFR include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Personally Identifiable Information;

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiff's and Class Members' Personally Identifiable Information; and

d. failing to recognize in a timely manner that Plaintiff's and other Class Members' Personally Identifiable Information had been compromised.

83. It was foreseeable that AFR's failure to use reasonable measures to protect and monitor the security of Personally Identifiable Information would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

84. It was therefore foreseeable that the failure to adequately safeguard Personally Identifiable Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

85. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that AFR's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

COUNT II

NEGLIGENCE PER SE

86. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

87. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade

Commission ("FTC"), the unfair act or practice by companies such as AFR of failing to use reasonable measures to protect Personally Identifiable Information. Various FTC publications and orders also form the basis of AFR's duty.

88. AFR violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personally Identifiable Information and not complying with industry standards.

89. AFR's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

90. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

91. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

92. As a direct and proximate result of AFR's negligence, Plaintiff and Class Members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III

BREACH OF IMPLIED CONTRACT

93. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

94. When Plaintiff and Class Members paid money and provided their Personally Identifiable Information to AFR in exchange for goods or services, they entered into implied

contracts with AFR pursuant to which AFR agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

95. AFR solicited and invited prospective customers to provide their PII as part of its regular business practices. These individuals accepted AFR's offers and provided their Information to AFR. In entering into such implied contracts, Plaintiff and the Class assumed that AFR's data security practices and policies were reasonable and consistent with industry standards, and that AFR would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

96. Plaintiff and the Class would not have provided and entrusted their Information to AFR in the absence of the implied contract between them and AFR to keep the information secure.

97. Plaintiff and the Class fully performed their obligations under the implied contracts with AFR.

98. AFR breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

99. As a direct and proximate result of AFR's breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein. .

COUNT IV

UNJUST ENRICHMENT

100. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

101. Plaintiff and Class Members conferred a monetary benefit on AFR in the form of monetary payments—made to AFR directly or indirectly.

102. AFR collected, maintained, and stored the Personally Identifiable Information of Plaintiff and Class Members and, as such, Defendant AFR had knowledge of the monetary benefits conferred by the consumers that use AFR's services (like Plaintiff and Class Members).

103. The money that consumers that use AFR's services paid to AFR should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' Personally Identifiable Information.

104. Defendant AFR failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive Personally Identifiable Information, as evidenced by the Data Breach.

105. As a result of Defendant AFR's failure to implement data security practices, procedures, and programs to secure sensitive Personally Identifiable Information, Plaintiff and Class Members suffered actual damages in an amount of the savings and costs Defendant AFR reasonably and contractually should have expended on data security measures to secure Plaintiff's Personally Identifiable Information.

106. Under principles of equity and good conscience, Defendant AFR should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant AFR failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' Personally Identifiable Information and that AFR customers paid for.

107. As a direct and proximate result of Defendant AFR's decision to profit rather than provide adequate security, and Defendant AFR's resultant disclosures of Plaintiff and Class Members' Personally Identifiable Information, Plaintiff and Class Members suffered and continue

to suffer considerable injuries in the forms of attempted identity theft, time and expenses mitigating harms, diminished value of Personally Identifiable Information, loss of privacy, and an increased risk of harm.

COUNT V

108. Plaintiff realleges and incorporates by reference all preceding parahraphs as if fully set forth herein.

109. The New Jersey Consumer Fraud Act (New Jersey CFA) makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby." N.J. STAT. ANN. § 56:8-2.

110. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. continued gathering and storage of PII, and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the data breach; and,

d. continued gathering and storage of PII, and other personal information after Defendant knew or should have known of the Ransomware Attack and before Defendant allegedly remediated the data security incident.

111. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act, the Gramm- Leach-Bliley Act, and the New Jersey CFA.

112. The foregoing deceptive acts and practices were directed at New Jersey consumers/purchasers.

113. Defendant, Plaintiff, and Class Members are "persons" within the meaning of N.J. STAT. ANN. § 56:8-1(d).

114. Defendant engaged in "sales" of "merchandise" within the meaning of N.J. STAT. ANN. § 56:8-1(c), (d).

115. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the financial services provided, specifically as to the safety and security of PII, and other personal and private information, to induce consumers to purchase the same.

116. Defendant's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiff and members of the Class, would attach importance to in making their purchasing decisions or conducting themselves regarding the purchase of services from Defendant.

117. Plaintiff and Class Members are New Jersey consumers who made payments to Defendant for the furnishing of financial services that were primarily for personal, family, or household purposes.

118. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of services to consumers, including Plaintiff and Class Members. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering to sell, and furnishing services to consumers in the State of New Jersey. As a direct and proximate result of Defendant's multiple, separate violations of N.J. STAT. ANN. § 56:8-2, Plaintiff and the Class Members suffered damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Ransomware Attack for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

119. Also as a direct result of Defendant's violation of the New Jersey Consumer Fraud Act, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen their data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members. Plaintiff and Class Members were injured because: a) they would not have purchased services from Defendant had they known the true nature and character of Defendant's data security practices; b) Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and c) Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

120. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

121. On behalf of themselves and other members of the Class, Plaintiff is entitled to recover legal and/or equitable relief, including an order enjoining Defendants' unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J. STAT. ANN. § 56:8-19, and any other just and appropriate relief.

VII. PRAYER FOR RELIEF

122. WHEREFORE, Plaintiff prays for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiff and his counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Personally Identifiable Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to utilize appropriate methods and

policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personally Identifiable Information compromised by the Data Breach.

VIII. JURY TRIAL DEMAND

123. Jury trial is demanded by Plaintiff and members of the putative Class.

Date: March 29, 2022

Respectfully Submitted,

/s/ *Victoria Maniatis*
Victoria Maniatis
Blake Hunter Yagman*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (212) 594-5300
vmaniatis@milberg.com
byagman@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

**pro hac vice forthcoming*